

REMARKS

In the Official Action mailed on **April 7, 2005** the Examiner reviewed claims 1-41, 50-52, and 61. The specification was objected to because of informalities. Claims 40 and 51 were objected to as being dependent upon a rejected base claim. Claims 41 and 52 were rejected under 35 U.S.C. §112 as failing to particularly point out and distinctly claim the subject matter which the Applicant regards as the invention. Claims 1-6, 8-9, 13-15, 19-24, 26-27, 31-33, and 37-38 were rejected under 35 U.S.C. §102(e) as being anticipated Gligor (USPub 2001/0033656, hereinafter "Gligor"). Claims 7 and 25 were rejected under 35 U.S.C. §103(a) as being unpatentable over Gligor in view of Press, (*Numerical Recipes in C: The Art of Scientific Computing*, 1992, Cambridge University Press, hereinafter "Press). Claims 10, 12, 16, 18, 28, 30, 34, and 36 were rejected under 35 U.S.C. §103(a) as being unpatentable over Gligor in further view of Jutla (*Encryption Modes with Almost Free Message Integrity*, August 2000, hereinafter "Jutla"). Claims 11, 17, 29, 35, 39, 50, and 61 were rejected under 35 U.S.C. §103(a) as being unpatentable over Gligor in view of Jutla in further view of Menezes (*Handbook of Applied Cryptography*, 1997, CRC Press Pages 321-383, hereinafter "Menezes).

Objection to the Specification

The specification was objected to because of informalities.

Applicant has amended the specification to correct the informalities noted by the Examiner. No new matter has been added.

Rejections under 35 U.S.C. §102(e), 35 U.S.C. §102(e), and 35 U.S.C. §103(a)

Claims 41 and 52 were rejected as failing to particularly point out and distinctly claim the subject matter which the Applicant regards as the invention. Claims 1-6, 8-9, 13-15, 19-24, 26-27, 31-33, and 37-38 were rejected as being

anticipated Gligor. Claims 7 and 25 were rejected as being unpatentable over Gligor in view of Press. Claims 10, 12, 16, 18, 28, 30, 34, and 36 were rejected as being unpatentable over Gligor in further view of Jutla. Claims 11, 17, 29, 35, 39, 50, and 61 were rejected as being unpatentable over Gligor in view of Jutla in further view of Menezes. Claims 40 and 51 were objected to as being dependent upon a rejected base claim.

Applicant has deleted claims 1-38, 41, 52, and 61 without prejudice.

Claims 40 and 51 were objected to as being dependent upon a rejected base claim.

Applicant has added new claims 67 and 68, which are merged versions of claims 39 and 40, and 50 and 51, respectively. Claims 39-40 and 50-51 have been canceled without prejudice.


Applicant has also added new claims 69-70. No new matter has been added.

Hence, Applicant respectfully submits that independent claims 67-70 are in condition for allowance.

CONCLUSION

It is submitted that the present application is presently in form for allowance. Such action is respectfully requested.

Respectfully submitted,

By 
Edward J. Grundler
Registration No. 47,615

Date: 01 July 2005

Edward J. Grundler
PARK, VAUGHAN & FLEMING LLP
2820 Fifth Street
Davis, CA 95616-7759
Tel: (530) 759-1663
FAX: (530) 759-1665